Energy 2003:
What? Me vulnerable?

Highly Reliable Power Systems: Myth or Legend?

August 18, 2003
Wyndham Palace Resort and Spa
Lake Buena Vista, Florida

Stephen Fairfax
President, MTechnology, Inc.

MTechnology, Inc. 2 Central Street Saxonville, MA 01701
(508) 778-6260; fax (508) 788-6233 fairfax@mtechnology.net

Outline

Introduction
Electric power reliability
Probabilistic Risk Assessment
Case Studies

Introduction to MTechnology

- Consulting Engineers
- Founded 1996
- Applied Probabilistic Risk Assessment:
  - Enterprise Data Centers
  - Hospitals, Bio-Medical Research Facilities
  - Distributed Generation for Reliability
    - First National Bank of Omaha
    - Harvard Medical School / Merck & Co.
    - Fidelity (in progress)
  - OEMs, A&E firms, end users

Electric Power Reliability

- Reliability: The probability that a system or component will operate for a given time
  - Can be function of time, events, environment
  - Reliability tends towards 0 (all things fail)
  - $R = 1 - P_f$ (Probability of Failure)
- What constitutes a power failure?
  - Most electric utilities: no power for >1 minute
  - Most computers: no power for > 0.08 seconds
  - Heart/lung machine, ventilator: ?

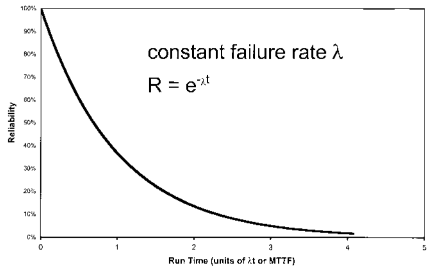
Definitions of Power Outage

- Computer Power:
  - At device level: sub-nanosecond
  - At system level: 1/2 cycle, 0.008 seconds
  - CBEMA and ANSI/IEEE C62.41-1991
- Utility power
  - Most utilities don't log interruptions <1 minute,
    - some start at 5 minutes
  - Many don't count outages in bad storms in published availability figures
  - Routine switch and fault-clearing cause 1/2 to 10-cycle upsets, reclosers deliberately interrupt for seconds

Electric Power Reliability

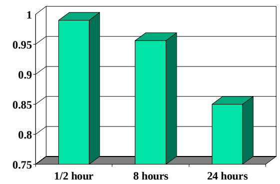
- Reliability varies widely
  - Electric utility to utility
  - Within one utility territory
  - From year to year at one location
- "Good" utility reliability
  - 2-3 outages > 1 minute, total ~ 60 minutes/year
  - 12-20 momentary outages < 1 minute / year
  - 30-40 sags, surges, other "power quality events"

Chart of Reliability(t)



Reliability Example

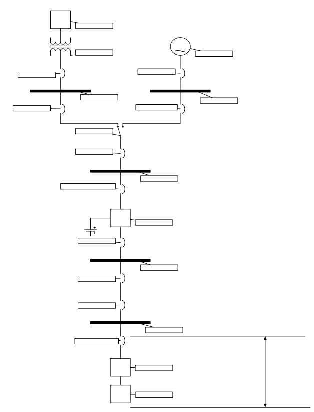
Reliability (Start, Load and Run) of Emergency Diesel Generators



Emergency Diesel Engine Generator Power System Reliability 1987-1993 Grant, G.M., et al., Idaho National Engineering Laboratory, INEL-95/0035, February 1996

“Premium Power” Protection

- Utility (sometimes 2 feeders)
- Standby diesel engine/generator(s)
- Uninterruptible Power Supply (UPS)
- Battery bank rated 10-40 minutes
- Automatic Transfer Switch (ATS)
- Fuel
- <u>People</u> to operate, maintain, repair



Summary of PRA Analysis of Example Power System

Mission Duration	1 Year	5 Years	10 Years
Probability of Failure	9.6%	41%	66%

Failure = Loss of Power for > 0.08 seconds

Probabilistic Risk Assessment

- Origins in understanding rocket failures
- Developed by military, aerospace, civilian nuclear power
- Constructs mathematical models of complex systems
  - Use knowledge of component failures to predict system failures
  - Can be applied to systems under design, compare proposed upgrades
  - Extended to risk-informed maintenance, effects of management policies, human error

Characteristics of PRA

- Basis in science, engineering, fact. Defensible. Falsifiable.
- Demands scrutiny of the entire life-cycle
  - design (logic, math, knowledge, review)
  - manufacture
  - operation
  - maintenance and repair
  - data gathering, review, publication
- Extreme care with definitions, assumptions, language
- Constant pursuit of root causes, common-cause failures, and relevant data

Why PRA?

- Difficult, dangerous to determine reliability by measuring failures
  - Highly reliable systems rarely fail
  - Results of failure increasingly unacceptable
- Evaluation of new and existing systems, alternatives
  - Risk/reward ratios, component sensitivity
  - Unintended interactions in complex systems
- Science-based approach avoids pitfalls
  - Answers appeals to anecdote, experience
  - Avoids excessive reliance on "worst-case" scenarios
- Human Reliability Analysis (HRA) evaluates operability, quantifies risk of human error, estimates effects of improved training, aids, design
- Provides rich, quantitative, useful results
  - Component contributions to risk
  - Confidence limits, best and worst cases
  - Effects of human error, aging equipment, test policy
  - Graphical aids to understanding complex systems

Why PRA?

- 7x24 Industry standard practice is to characterize systems by redundancy:
  N, N+1, 2N, 2N+2
- Redundancy provides no guidance as to relative contribution of each component to overall risk
- Impossible to allocate limited resources optimally, rationally, or defensibly
- PRA quantifies risks, focuses capital and operating resources where ROI is greatest

Typical Data Center Failure Profile

- Based on recent data center PRA w/1200 kW critical load, dual-cord equipment
- Fraction of failures caused by:
  - ATS, sensors, cables: 30%
  - Circuit breakers: 40%
  - UPS Failure: 20%
  - Balance of System: 10%
- Probability of failure exceeds 70% in 20 years

PRA is an Engineering Tool

- Quantifies probability of failure, availability
- Identifies most critical systems
- Estimates improvement possible via
  - Additional equipment e.g. N+1 vs 2N
  - Premium components
  - Targeted maintenance/surveillance

PRA is a Management Tool

- Provides guidance for review, decisions
- Quantifies risk (probability & consequences)
- Quantitative confidence limits/worst-case results
- Measures effectiveness of proposed solutions
- Focuses attention, resources on critical areas
- Guidance for least-harmful reductions, cuts
- Graphical aids for presentation of complex relationships

PRA Adds Value

- Choosing the best design is always less expensive than changing installed systems.
- Reduce redundancy where it contributes least: no need for rigid 2N vs N+1 rule.
- Focus commissioning and maintenance activities where they do the most good and least harm.
- Place facility decisions on same quantitative base as other business process decisions.
- Powerful tool for communication to management, stakeholders, designers, and operators.

Case Studies

- Effects of Power Failure
  - Integrated Circuit factory
  - Biomedical research facility
  - Hospitals
- PRA results
  - First National Bank of Omaha
  - Harvard Medical School/Merck & Co.

Consequences of Electric Power Failure

- Integrated Circuit Fabrication Facility
  - Chandler, AZ
  - Utility switches capacitor bank
    - standard practice on transmission system
  - Facility power protection apparatus failed
  - 4-second outage on 1/2 of plant systems
  - 34 hours to resume production

Consequences of Electric Power Failure

- Columbia Presbyterian Medical Center
  - 19-hour Manhattan blackout summer 1999
  - 3 of 4 diesels started, all failed in less than 4 hours
  - Freezers of irreplaceable tissue samples, research materials, 20-year collections lost
  - Short outages reset all computers, computerized instruments with unpredictable effects

Consequences of Electric Power Failure

- Houston Hospitals, Medical Center, Medical School
  - June 5-12 2001: Tropical Storm Allison: torrential rains, flooding, $2+ billion damages
  - Memorial Hermann Hospital lost all power, evacuated 540 patients, 4 died
    - Generators moved from basement after previous flood
    - Transfer switches, controls remain in basement
  - June 14: emergency rooms remain closed at Methodist Hospital and St. Luke's Episcopal Hospital, lack of power
  - Texas Medical Center, Baylor College of Medicine
    - 30,000 genetically engineered animals lost
    - Years of research data, cultures, specimens lost due to loss of refrigeration power

First National Bank of Omaha

- Major credit card processing center
  - Real-time processing for VISA
- Multiple failures of standard UPS systems
  - $ millions in damages to FBNO, customers
- Retained MTech for evaluation of on-site distributed generation proposal

First National Bank of Omaha

- Unique contract provisions specified minimum 99.999% availability
  - Equivalent to 10% probability of failure in 20 year operating life
- Primary power: 4 fuel cells, any 2 of 4
- Backup 1: 2 diesel generators
- Backup 2: 2 utility feeds
- 2 flywheel batteries, 2 rotary UPS

First National Bank of Omaha

- Results
  - PRA calculated availability ~ 99.9999%
    - Unavailability <10^{-6}
  - Identified most sensitive component
    - Not obvious
    - On-site spare decreases risk of failure 10x
  - Quantified risk/reward of operating policies
  - Operating since May 1999
    - All components have failed, no system failures

Harvard Medical School Merck & Co.

- Side-by-side 400,000 sq. ft. biomedical research facilities under construction in Boston's Longwood Medical Area
- Massachusetts Renewable Energy Trust awarded planning grant
- MTechnology performed economic, feasibility, PRA analysis of proposed 1 MW fuel-cell based facility
- Unique opportunity for public, private, and academic collaboration

HMS/Merck results

- 2 fixed-price proposals by qualified vendors
- Each suggested at least 2 alternatives
- All alternatives utilized fuel cells
- Best case: <1% risk of failure in 10 years
- Worst case: >90% risk of failure
- Same fuel cells, different architecture
- High site-specific costs, reduced subsidies
- Construction not likely

Summary

- Review of electric power reliability
- Benefits of PRA
  - Rational resource allocation
  - Informed risk management
- Case studies
  - Effects of power outages
    - $ millions in damages, injuries, deaths
  - FBNO and HMS/Merck distributed generation